Matrix Fields over the Integers Modulo m

Jacob T. B. Beard, Jr.*
The University of Texas at Arlington

and

Robert M. McConnel
The University of Tennessee, Knoxville, Tennessee

Submitted by Hans Schneider

ABSTRACT

Let Zm denote the ring of integers *modulo* m, and let $(Zm)_n$ denote the complete ring of all $n \times n$ matrices over Zm under the usual matrix addition and multiplication. The primary purposes of this paper are to characterize and count all subfields of the ring $(Zm)_n$. Related results are given on field extensions in $(Zm)_n$ of subfields of $(Zm)_n$. Partial results on subfields of $(R)_n$ when R is an arbitrary finite commutative ring with identity are also given. Having basic significance, a partial characterization of rings containing division rings is obtained.

1. INTRODUCTION

Let R be a ring with identity, and let $(R)_n$ denote the complete matrix ring of all $n \times n$ matrices over R under the usual matrix addition and multiplication. A subring M of $(R)_n$ is called a *matrix field* over R if and only if M is itself a field. For convenience we refer to a matrix field over R as a *subfield* of the ring $(R)_n$. *The reader is cautioned that we do not require the identity of a subfield of* $(R)_n$ *to be the identity of the ring* $(R)_n$. We are interested in characterizing up to similarity all subfields of $(R)_n$ and counting the distinct subfields of $(R)_n$ for finite rings R. Beard [2, 3] initiated the attack with a characterization of all subfields of $(F)_n$ whenever the field F has arbitrary characteristic and is a finite extension of its prime subfield, and counted the distinct subfields of $(\mathrm{GF}(q))_n$ in [4], $\mathrm{GF}(q)$ denoting the Galois

*This author was partially supported by an Organized Research Grant from the University of Texas at Arlington.

field of order $q = p^d$. The primary purposes of this paper are to characterize and count the subfields of $(Zm)_n$, where Zm denotes the ring of integers modulo m. Our characterization is given in Sec. 3, and the number $N(m,n)$ of distinct subfields of $(Zm)_n$ is given in Sec. 4. In Sec. 5 we give results on extending subfields of $(Zm)_n$ in $(Zm)_n$ and on the structure of the set Z_n of all subfields of $(Zm)_n$. Section 6 is devoted to partial results on matrix fields over arbitrary finite commutative rings with identity.

2. RINGS CONTAINING DIVISION RINGS

Let R be an arbitrary ring, and let $S_n(R)$ denote the subring of all $n \times n$ scalar matrices $\operatorname{diag}|\alpha, \ldots, \alpha|$, $\alpha \in R$. (No confusion will result from the use of $|\alpha_{ij}|$ to denote a matrix, since determinants are not used.) It is basic knowledge that T is a subring (ideal) of R if and only if $(T)_n$ is a subring (ideal) of $(R)_n$. Indeed, if R has an identity, then *every* ideal in $(R)_n$ has the form $(T)_n$, where T is an ideal of R [7, p. 37]. While none of the exact analogues of these statements hold for subfields or division subrings of R and $(R)_n$, trivially F is a subfield (division subring) of R if and only if $S_n(F)$ is a subfield (division subring) of $(R)_n$. The first result of this section was anticipated in [2; Theorem 1], where it was argued that the ring $(Z)_n$ of integral matrices contains no subfields. We recall that the matrices $A, B \in (R)_n$ are similar over R if and only if R has an identity and there exists an invertible matrix $P \in (R)_n$ such that $A = PBP^{-1}$. If $A \in (R)_n$ is similar over R to a diagonal matrix, we say that A is *diagonable over* R.

THEOREM 1. *Let R be a ring with identity for which each idempotent matrix in $(R)_n$ is diagonable over R. Then R contains a division ring if and only if $(R)_n$ contains a division ring.*

Proof. The necessity is immediate, as remarked above. Hence assume R and $(R)_n$ satisfy the hypothesis, and suppose M_1 is a division subring of $(R)_n$. The division ring M_1 has an identity—call it I_1—and by hypothesis we have $PI_1P^{-1} = I = \operatorname{diag}|e_1, \ldots, e_n|$ for some invertible matrix $P \in (R)_n$. Since the conjugation of $(R)_n$ by P induces a ring automorphism (similarity transformation) of $(R)_n$, it follows that $M = PM_1P^{-1}$ is a division subring of $(R)_n$ and has I as its identity. Hence I is idempotent and non-zero, so that each e_i is idempotent and at least one e_i is non-zero, say $e_j \neq 0$. Let D be the integral domain in M generated by I. Then $D = \{mI : m \in Z\}$, where Z denotes the integers. Let $A = \operatorname{diag}|a_1, \ldots, a_n| \in D$ be a non-zero matrix. Then $A \in M$, and

A is invertible in M; hence there exists a unique matrix $A^{-1} \in M$ such that $AA^{-1} = I$. Note that for $A^{-1} = |\alpha_{ij}|$, the (j,j)-entry in AA^{-1} is $a_j \alpha_{jj}$. Thus if $a_j = 0$, then $e_j = 0$, a contradiction. Hence every non-zero matrix in D has a non-zero entry in its (j,j)-position. Denote e_j by e, and let (e) denote the subring of R generated by e. As e is an idempotent of R, $(e) = \{me : m \in Z\}$. If $a \in (e)$ occurred as the jth diagonal entry of both A_1 and A_2 in D, then $A_1 - A_2 \in D$ and has 0 as its jth diagonal entry. If $A_1 \neq A_2$, then $A_1 - A_2$ is invertible in M. Since this leads to the contradiction that $e = 0$, every element of (e) occurs as an a_j in some $A = \operatorname{diag}|a_1, \ldots, a_n| \in D$ and occurs in only one such matrix $A \in D$. As D is an integral domain, it now follows easily that (e) is an integral domain. For each $a \in (e)$, let $A(a)$ be the unique matrix $A(a) = \operatorname{diag}|a_1, \ldots, a_n| \in D$ having $a_j = a$, and note that the projection of $A(a)$ onto a defines an isomorphism of D onto (e). For each $a \in (e)$, $a \neq 0$, let $A(a)^{-1}$ be the unique inverse in M of $A(a)$. Observe that since D is commutative, $A(a)^{-1}$ and $A(b)^{-1}$ commute whenever $a, b \in (e)$ are non-zero. Moreover, $A(a)$ and $A(b)^{-1}$ commute whenever $a, b \in (e)$ and $b \neq 0$. Hence

$$M' = \{A(a)A(b)^{-1} : a, b \in (e),\ b \neq 0\}$$

is the prime subfield of the division ring M, and thus M' is the quotient field in M of D. Setting $A(b)^{-1} = |\alpha_{ij}(b)|$, one observes that $a\alpha_{jj}(b) = \alpha_{jj}(b)a$ follows by comparing the (j,j)-entries in the identity $A(a)A(b)^{-1} = A(b)^{-1}A(a)$, which one obtains from the diagonal form of $A(a)$ and the above remarks. In particular, $b\alpha_{jj}(b) = e = \alpha_{jj}(b)b$. Set $b^{-1} = \alpha_{jj}(b)$ and define

$$F = \{ab^{-1} : a, b \in (e),\ b \neq 0\}.$$

We show that F is a quotient field in R for the integral domain (e). Let $\phi : M' \to F$ be defined by

$$\phi(A(a)A(b)^{-1}) = ab^{-1}, \qquad A(a)A(b)^{-1} \in M';$$

i.e., ϕ is the projection of $A(a)A(b)^{-1}$ onto its (j,j)-entry. Clearly, ϕ maps M' onto F. Let $A(a_1)A(b_1)^{-1}, A(a_2)A(b_2)^{-1} \in M'$. Thus we have

$$\phi(A(a_1)A(b_1)^{-1} + A(a_2)A(b_2)^{-1}) = a_1 b_1^{-1} + a_2 b_2^{-1}$$

$$= \phi(A(a_1)A(b_1)^{-1}) + \phi(A(a_2)A(b_2)^{-1}). \quad (2.1)$$

Since M' is a field,

$$\begin{aligned}\phi\big(A(a_1)A(b_1)^{-1}A(a_2)A(b_2)^{-1}\big) &= \phi\big(A(a_1)A(a_2)(A(b_2)A(b_1))^{-1}\big)\\ &= a_1a_2(b_2b_1)^{-1}\\ &= a_1b_1^{-1}a_2b_2^{-1}\\ &= \phi\big(A(a_1)A(b_1)^{-1}\big)\phi\big(A(a_2)A(b_2)^{-1}\big). \blacksquare\end{aligned} \tag{2.2}$$

COROLLARY *Let R be a ring with identity and M a division subring of $(R)_n$ having identity $I=\operatorname{diag}|e_1,\ldots,e_n|$. Then for each $e_j\neq 0$, $1\leqslant j\leqslant n$, R contains a quotient field F_j of the integral domain (e_j), and the F_j are isomorphic.*

Steger [8] has called a commutative ring R with identity an ID-ring if and only if each idempotent matrix in $(R)_n$ is diagonable over R for $n=1,2,\ldots$. Thus the class of rings characterized in Theorem 1 contains those ID-rings R containing division subrings.

THEOREM 2. *Let R be an* ID*-ring and let n be an arbitrary positive integer. Then R contains a division ring if and only if $(R)_n$ contains a division ring.*

We observe that if each (idempotent) matrix in $(R)_n$ is diagonable over R, then each (idempotent) matrix in $(R)_k$ is diagonable over R for $1\leqslant k\leqslant n$. Steger's definition [8] of ID-rings allows that perhaps the conclusion does not follow for $k>n$, and this remains an open question. Nonetheless, we are able to obtain

THEOREM 3. *Let R be a ring with identity, and suppose there exists an integer $n\geqslant 2$ such that each idempotent matrix in $(R)_n$ is diagonable over R. The following are equivalent.*

(i) *R contains a division ring.*
(ii) *R contains a field.*
(iii) *$(R)_n$ contains a division ring.*
(iv) *$(R)_n$ contains a field.*
(v) *$(R)_m$ contains a division ring for each integer $m\geqslant 1$.*
(vi) *$(R)_m$ contains a field for each integer $m\geqslant 1$.*

Proof. Previously used basic arguments yield (v)→(vi)→(i)→(ii)→(iii)→(iv); hence we show (iv)→(v). If $(R)_n$ contains a field, then R contains a field F by Theorem 1. Hence for any $m \geqslant 1$, $S_m(F)$ is a division subring of $(R)_m$.

3. SUBFIELDS OF $(Zm)_n$

The results in [2–4] lead us to consider subfields, if any, of $(R)_n$ whenever R is a finite commutative ring with identity and has a composite characteristic. We are primarily interested in matrix fields over the ring generated by the identity of such a ring R; hence in this section we take R to be isomorphic to Zm. Of primary concern is the existence of a suitable canonical form under similarity for the idempotent matrices in $(R)_n$. Davis [6, p. 56] has obtained the needed partial identity matrix for idempotent matrices over Zm, while Steger [8, Theorem 4] obtained a suitable form for the full class of ID-rings. We appeal to Davis here and to Steger in Sec. 6, recognizing that Steger's result is applicable in this section also.

Let $m > 1$ have prime power decomposition

$$m = m_1 m_2 \cdots m_l \tag{3.1}$$

where $m_i = p_i^{\alpha(i)}$ and the primes p_i are distinct. From the Chinese remainder theorem, it easily follows that Zm is the ring direct sum of the Zm_i. Hence Zm contains ideals isomorphic to the Zm_i—call them Zm_i—and

$$Zm = Zm_1 \oplus \cdots \oplus Zm_l. \tag{3.2}$$

From the opening facts of Sec. 2 we have

$$(Zm)_n = (Zm_1)_n \oplus \cdots \oplus (Zm_l)_n. \tag{3.3}$$

Let $A, B \in (Zm)_n$. For $A = A_1 + \cdots + A_l$ and $B = B_1 + \cdots + B_l$, where $A_i, B_i \in (Zm_i)_n$ for $1 \leqslant i \leqslant l$, we write $A_1 + \cdots + A_l \equiv B_1 + \cdots + B_l \pmod{m}$ to mean $A_i \equiv B_i \pmod{m_i}$ for $1 \leqslant i \leqslant l$. The reader will not be confused if $(Zm)_n$ as in (3.3) is associated with the isomorphic copy $(Zm)_n \cong (Zm_1)_n \times \cdots \times (Zm_l)_n$, in which case the operations of addition and multiplication are performed componentwise. Our initial characterization of the subfields of $(Zm)_n$ will follow quickly from three lemmas.

LEMMA 4. *Let m have factorization given by* (3.1), *and let I be a non-zero idempotent in $(Zm)_n$. Then the subring (I) of $(Zm)_n$ generated by I has order $o(I)$ given by*

$$o(I) = \prod_i m_i,$$

where the product is taken over all i such that $I \not\equiv 0_n \pmod{m_i}$.

Proof. Let $I \in (Zm)_n$ be a non-zero idempotent. Then I can be written uniquely as $I = A_1 + \cdots + A_l$, where $A_1 \in (Zm_i)_n$ for $1 \leqslant i \leqslant l$. Furthermore, each A_i is idempotent in $(Zm_i)_n$, and $A_i \neq 0_n$ for at least one i, $1 \leqslant i \leqslant l$. We can assume without loss of generality that for some s satisfying $1 \leqslant s \leqslant l$ we have $A_i \neq 0_n$ if and only if $1 \leqslant i \leqslant s$. Davis [6;56] has shown that for each i, $1 \leqslant i \leqslant s$, A_i is similar over Zm_i to a partial identity matrix $C_i = \operatorname{diag}|I_i, 0_{n-t}|$, where I_i is the identity of the ideal $(Zm_i)_t$, t is a rank function of A_i satisfying $0 < t \leqslant n$, and 0_{n-t} is the zero matrix of order $n-t$. Thus for each i, $1 \leqslant i \leqslant s$, there exists an invertible matrix $Q_i \in (Zm_i)_n$ such that

$$Q_i A_i Q_i^{-1} \equiv C_i \pmod{m_i}.$$

Let $Q \in (Zm)_n$ be the matrix given by

$$Q = Q_1 + \cdots + A_s + I_{(s+1)} + \cdots + I_l,$$

where I_i is the identity of $(Zm_i)_n$ for $s < i \leqslant l$. The canonical projections of Q are all invertible; hence Q is invertible in $(Zm)_n$, and we let

$$\begin{aligned} I' &\equiv QIQ^{-1} \pmod{m} \\ &\equiv C_1 + \cdots + C_s + 0_n + \cdots + 0_n \pmod{m} \\ &\equiv C_1 + \cdots + C_s \pmod{m}. \end{aligned} \tag{3.4}$$

Then $(I) \cong (I')$, since $Q(I)Q^{-1} = (I')$, and our lemma follows, since $(p_i, p_j) = 1$ for $i \neq j$.

LEMMA 5. *Let $I \in (Zm)_n$ be a non-zero idempotent. If I is contained in a subfield of $(Zm)_n$, then (I) has order p for some prime $p \| m$. Conversely, if (I) has prime order p, then $p \| m$, and I is contained in a subfield of $(Zm)_n$.*

From Lemma 5 and the proof of Lemma 4 we obtain

LEMMA 6. *Let $I \in (Zm)_n$ be a non-zero idempotent. Then I is contained in a subfield of $(Zm)_n$ if and only if $I \not\equiv 0_n \pmod{p}$ for precisely one prime $p|m$ and for this prime, $p \| m$.*

Our initial characterization now follows from Lemma 6.

THEOREM 7. *Let M be a subring of $(Zm)_n$, with $(Zm)_n$ as described by (3.3). Then M is a subfield of $(Zm)_n$ if and only if M is a subfield of an ideal $(Zp)_n$ of $(Zm)_n$ for some prime $p \| m$.*

Proof. The containment $M \subset (Zp)_n$ follows on considering the *additive* order of an arbitrary matrix $A \in M$, where $I \not\equiv 0_n \pmod{p}$, I the identity of M. ∎

We refer the reader to [2] for a thorough discussion of the subfields of $(Zp)_n$, and in Sec. 5 we will give several analogous results as they extend to subfields of $(Zm)_n$. We conclude this section with a constructive characterization of the subfields of $(Zm)_n$ afforded by Theorem 7 above and [2, Theorems 2, 3]. The notation and terminology used there is the obvious extension of that in [2]. In particular, $C(f(x))$ denotes the companion matrix of the monic polynomial $f(x)$.

THEOREM 8. *Let M be a subring of $(Zm)_n$ having rank n. Then M is a subfield of $(Zm)_n$ if and only if M is similar over Zm to the matrix field k-sum$(S_d(Zp)[C(f(x))])$ for some prime $p \| m$ and for some prime polynomial $f(x) \in Zp[x]$ of degree d, where $n = kd$.*

THEOREM 9. *Let M be any subring of $(Zm)_n$ having rank $r < n$. Then M is a subfield of $(Zm)_n$ if and only if M is similar over Zm to a matrix field $1°$-sum$(M'; n-r, 0)$, where M' is a subfield of $(Zp)_r$ for some prime $p \| m$ and M' has rank r.*

4. THE NUMBER $N(m,n)$

Beard [4, Theorem 9] gives the number $N(p,n,d,r)$ of distinct subfields of $(Zp)_n$ having order p^d and rank r as

$$N(p,n,d,r) = \frac{1}{d} \frac{g(1,n)}{g(1,n-r)\, g(d,r/d)} \tag{4.1}$$

whenever $d|r$, where $g(s,t)$ is the number of non-singular matrices of order t over $\mathrm{GF}(p^s)$ and $g(s,0)=1$. If $d\nmid r$, then $N(p,n,d,r)=0$, so that the number $N(p,n)$ of distinct subfields of $(Zp)_n$ is then [4; Theorem 10]

$$N(p,n)=\sum_{r=1}^{n}\sum_{d|r}\frac{1}{d}\,\frac{g(1,n)}{g(1,n-r)\,g(d,r/d)}\,.$$

Our next two results follow immediately from (4.1), (4.2), and Theorem 7. The value of $g(s,t)$ is well known as $g(s,t)=\prod_{i=0}^{t-1}(p^{st}-p^{si})$, the number of non-singular matrices of order t over $\mathrm{GF}(p^s)$, and $g(s,0)=1$.

THEOREM 10. *The number $N(p,n,d,r)$ of distinct subfields of $(Zm)_n$ having order p^d and rank r is given by*

$$N(p,n,d,r)=\frac{1}{d}\,\frac{g(1,n)}{g(1,n-r)\,g(d,r/d)} \tag{4.3}$$

whenever $p\|m$ and $d|r$. Otherwise, $N(p,n,d,r)=0$.

THEOREM 11. *The number $N(m,n)$ of distinct subfields of $(Zm)_n$ is given by*

$$N(m,n)=\sum_{p\|m}\sum_{r=1}^{n}\sum_{d|r}\frac{1}{d}\,\frac{g(p,1,n)}{g(p,1,n-r)\,g(p,d,r/d)}\,, \tag{4.4}$$

where $g(p,s,t)=\prod_{i=0}^{t-1}(p^{st}-p^{si})$ is the number of non-singular matrices of order t over $\mathrm{GF}(p^s)$ and $g(p,s,0)=1$.

5. RELATED RESULTS

Let Z_n denote the set of all subfields of $(Zm)_n$, and partially order Z_n under set inclusion whenever Z_n is non-empty. The results of [2, Sec. 4] all extend immediately as Theorems 12–16 below, due to Theorem 7 in Sec. 3.

THEOREM 12. *Each non-zero idempotent of $(Zm)_n$ which is incongruent to 0_n modulo p for precisely one prime $p\|m$ is contained in a unique prime subfield of $(Zm)_n$. No other non-zero idempotent of $(Zm)_n$ is contained in a subfield of $(Zm)_n$.*

THEOREM 13. *If $M' \in Z_n$ is a prime matrix field of rank r and if $M \in Z_n$ is any extension of M', then $[M:M'] \leqslant r$.*

THEOREM 14. *If $M \in Z_n$ has prime subfield M' and $[M:M'] = d$, then $1 \leqslant d \leqslant n$. Conversely, for each prime $p \| m$ and for each d satisfying $1 \leqslant d \leqslant n$, there exists a prime matrix field $M' \in Z_n$ (of order p) and a maximal extension $M \in Z_n$ of M' such that $[M:M'] = d$.*

THEOREM 15. *For each prime $p \| m$ and for any $M \in Z_n$ having characteristic p, rank r, and prime subfield M', there exists an extension $M'' \in Z_n$ of M such that $[M'':M'] = r$.*

THEOREM 16. *Let $F = \mathrm{GF}(q)$, $q = p^d$. Then F is represented as a maximal subfield of $(Zm)_n$ whenever $p \| m$ and $n \geqslant d$.*

Analogous to [4, Theorem 11] we have the following result.

THEOREM 17. *Any two subfields of $(Zm)_n$ having the same order and rank are similar over Zm.*

From Davis [6, p. 56], Theorem 8, Theorem 9, and Theorem 17 we obtain

THEOREM 18. *The number of similarity classes of subfields of $(Zm)_n$ is $\rho(m) \sum_{r=1}^{n} \tau(r)$, where $\rho(m)$ is the number of primes p such that $p \| m$ and $\tau(r)$ is the number of positive divisors of r.*

The following analog of the Sylow theorems comprises Theorems 13, 15, and 17 and (4.3) of Theorem 10.

THEOREM 19.

(i) *Any subfield of $(Zm)_n$ having rank r and characteristic p is contained in a maximal subfield of $(Zm)_n$ having order p^r.*

(ii) *Any two maximal subfields of $(Zm)_n$ having the same order are similar over Zm.*

(iii) *The number of (maximal) subfields of $(Zm)_n$ of any given order is zero or else it divides the order of the multiplicative group of non-singular matrices in $(Zm)_n$.*

Since any subfield M of $(Zm)_n$ is a subfield of $(Zp)_n$ for some p, it follows that for any matrix $A \in M$ the concepts of a rational canonical form for A over Zm and a rational canonical form (R.C.F.) for M over Zm present no

problems, and results analogous to those of Beard [5] in this vein extend immediately to the present case. For example, we state the following analog of [5, Theorem 3].

THEOREM 20. *Let M be a subfield of $(Zm)_n$ having rank r. Then there exists a subfield M' of $(Zm)_n$ such that M' is a* R.C.F. *for M over Zm. Furthermore, the canonical injection $\pi_r M'$ contains at most one non-scalar matrix in rational canonical form over Zm.*

6. SUBFIELDS OF $(R)_n$

For the remainder, R denotes a finite commutative ring with identity. Then R is uniquely decomposable (up to isomorphism and the ordering of the components) as a ring direct sum of finite local rings R_i [1, p. 90].

$$R = R_1 \oplus \cdots \oplus R_l. \tag{6.1}$$

As in Sec. 3, we consider the R_i as ideals of R and obtain the internal direct sum decomposition of $(R)_n$ as

$$(R)_n = (R_1)_n \oplus \cdots \oplus (R_l)_n. \tag{6.2}$$

Thus any matrix $A \in (R)_n$ has a unique representation $A = A_1 + \cdots + A_l$, where $A_i \in (R_i)_n$, and A is idempotent if and only if each A_i is idempotent. Since each R_i has a unique maximal ideal N_i and N_i is nilpotent, we have $R_i/N_i \cong \mathrm{GF}(p_i^{e(i)})$, and R_i has characteristic $p_i^{a(i)} = m_i$. Thus $Zm_i \subseteq R_i$ and $(Zm_i)_n \subseteq (R_i)_n$. Since R_i/N_i is a field, the only idempotents of R_i are 0 and 1, and we consider these as elements of Zm_i. By [8, Theorem 9] the R_i are ID-rings. Thus immediately from [8, Theorem 4] and the fact that 0, 1 are the only idempotents of R_i, each non-zero idempotent $A_i \in (R_i)_n$ is similar over R_i to a partial identity matrix $C_i = \mathrm{diag}|I_i, 0_{n-t}|$, as described earlier. Clearly then, any subfield of $(R_i)_n$ can be characterized up to similarity as a finite algebraic extension of a prime field of "scalar" matrices. Using either the arguments of Sec. 3, or the suggestion of the referee which is included in the following proof, we obtain our final results.

LEMMA 21. *Let $R = R_1 \oplus \cdots \oplus R_l$ be the direct sum of local rings R_i having characteristics $p_i^{a(i)}$, and let I be a non-zero idempotent in $(R)_n$. Then the subring (I) of $(R)_n$ generated by I has order $o(I)$ given by*

$$o(I) = \prod p^{b(p)}, \tag{6.3}$$

where $b(p)$ is the maximum of all $a(i)$ for which both $p_i = p$ and $I \not\equiv 0_n \pmod{R_i}$ or else $b(p) = 0$.

Proof. The result follows easily from the observation that if $A \in (R_i)_n$ has additive order less than $p_i^{a(i)}$, then $A \in (N_i)_n$ and hence is nilpotent. Thus any non-zero idempotent $I \in (R_i)_n$ has order $p_i^{a(i)}$. ■

THEOREM 22. *Let $I \in (R)_n$ be a non-zero idempotent, where R is the direct sum of local rings R_i having characteristics $p_i^{a(i)}$. Then I is contained in a (unique prime) subfield of $(R)_n$ if and only if there exists a prime p such that $p \| p_i^{a(i)}$ whenever $I \not\equiv 0_n \pmod{R_i}$.*

The preceding discussion indicates that any characterization of the subfields of $(R)_n$ would involve the π-diagonal rings utilized in [3] as well as monomorphic mappings among the components of R having the same prime characteristic. It appears, however, that more than these are involved.

REFERENCES

1 M. F. Atiyah and I. G. McDonald, *Introduction to Commutative Algebra*, Reading, Mass.: Addison-Wesley Publishing Company, 1969.
2 J. T. B. Beard, Jr., Matrix fields over prime fields, *Duke Math. J.* **39** (1972), 313–322.
3 J. T. B. Beard, Jr., Matrix fields over finite extensions of prime fields, *Duke Math. J.* **39** (1972), 475–484.
4 J. T. B. Beard, Jr., The number of matrix fields over GF(q), *Acta Arith.* **25** (1974), 315–329.
5 J. T. B. Beard, Jr., A rational canonical form for matrix fields, *Acta Arith.* **25** (1974), 331–335.
6 R. W. Davis, Certain matrix equations over rings of integers, *Duke Math. J.* **35** (1968), 49–59.
7 N. H. McCoy, *The Theory of Rings*, London: The Macmillan Company, 1964.
8 A. Steger, Diagonability of idempotent matrices, *Pac. J. Math.* **19** (1966), 535–542.

Received 6 November 1974; revised 17 July 1974